AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application claims indicated as cancelled:

1. (Currently Amended) A method for ~~protecting~~ controlling the transfer of data between a computer and an external device connected to a port of the computer, the method comprising the steps of:

a. receiving, by a module on the computer, a data portion during a data communication session between the computer and the external device, said external device connected to the computer and communicating therewith via a physical communication port;

b. analyzing, by said module, the data portion according to a protocol associated with the physical communication port;

c. determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached, wherein if no decision may be reached on whether to allow said data communication session, then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached, then proceeding to step 'd';

d. determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication session, wherein if said data communication session is to be allowed, then transferring the data portion with data stored in the associated buffer, if any exist, toward or from the physical communication port, and if said data communication session is not to be allowed, then modifying data transportation related to said data communication session.

2. (Previously Presented) The method of claim 1, wherein the step of modifying the data transportation comprises blocking the transportation.

3. (Previously Presented) The method of claim 1, wherein the step of modifying the data transportation comprises modifying the type of the transportation.

4. (Previously Presented) The method of claim 1, wherein the step of modifying the data transportation comprises modifying a status of a requested file.

5. (Previously Presented) The method of claim 1, wherein the step of modifying the data transportation comprises correcting the data according to the communication protocol.

6. (Original) The method of claim 1, wherein the physical communication port is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared.

7. (Original) The method of claim 1, wherein the physical communication port is a USB port.

8. (Original) The method of claim 1, wherein the physical communication port is wireless.

9. (Previously Presented) The method of claim 1, wherein the step of analyzing the data portion further comprising:

(i) determining whether additional processing based on a higher level protocol is required, wherein if additional processing is not required, then continuing at step 'c', otherwise continuing at step (ii); and

(ii) processing part of the data portion relevant to the higher level protocol according to the higher level protocol and returning to step (i).

10. (Previously Presented) The method of claim 9, wherein the step of analyzing the data portion comprises analyzing relevant to a higher level protocol that is associated with the external device.

11. (Previously Presented) The method of claim 10, wherein the data communication session is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols.

12. (Previously Presented) The method of claim 1, wherein the step of analyzing the data portion is performed in respect of the data stored in the associated buffer.

13. (Previously Presented) The method of claim 1, wherein the step of determining whether a decision on the data communication session may be reached is performed in respect of the data stored in the associated buffer.

14. (Previously Presented) The method of claim 1, wherein the step of determining whether to allow the data communication session is performed in respect of the data stored in the associated buffer.

15. (Previously Presented) The method of claim 1, wherein the step of receiving a data portion comprises receiving a data portion selected from a group consisting of packet and SCSI block.

16. (Previously Presented) The method of claim 1, wherein the step of receiving the data portion comprises obtaining the data portion by emulating a class driver.

17. (Previously Presented) The method of claim 1, wherein step of receiving the data portion comprises obtaining the data portion by emulating a filter module.

18. (Previously Presented) The method of claim 1, wherein the step of analyzing the data portion according to a protocol associated with the physical communication port further comprises:

i. parsing the data portion;

ii. reassembling the data; and

iii. analyzing the reassembled data.

19. (Previously Presented) The method of claim 1, wherein the step of determining whether to allow the communication session comprises reviewing a security policy.

20. (Previously Presented) The method of claim 1, wherein the step of determining whether to allow the communication session comprises examining the working environment in which the computer is operating and allowing the communication only if said computer is operating in one or more of certain working environments.

21. (Previously Presented) A system for protecting the transfer of data between a computer coupled to a private network and an external device, the system comprising:

a client agent installed on the computer, the client agent having an associated security policy;

a security manager communicatively coupled to the private network and operable to associate said security policy with the client agent;

wherein the client agent is operative to:

obtain at least a portion of a data transfer between a hardware device connected to the computer through a physical communication port of the computer;

analyze said at least a portion of the data transfer according to a communication protocol associated with the physical communication port; and

determine whether the data transfer is allowable based, at least in part, on the analysis of the at least a portion of the data transfer and the security policy, and, if not determining whether the data

transfer is allowable, then store the at least portion of the data transfer in a buffer associated with the data transfer and wait for a subsequent data portion and, if determining the data transfer is allowable, then transferring the at least a portion of the data transfer with data stored in the associated buffer, if any exist, toward or from the physical communication port.

22. (Original) The system of claim 21, wherein the security manager is operable to verify that the security policy is correct.

23. (Original) The system of claim 21, wherein the security policy includes a plurality of rules that at least define limits on data transfers during a communication session.

24. (Previously Presented) The system of claim 21, wherein the security policy includes a plurality of rules related to at least a content of the data portion and a type of an operation that can be performed during the communication session.

25. (Previously presented) The system of claim 21, wherein the security manager is operable to disable any communication with the computer unless the client agent associated with the computer is active.

26. (Previously Presented) The system of claim 21, wherein the physical communication ports is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared.

27. (Previously presented) The system of claim 21, wherein the physical communication ports is a USB port.

28. (Previously Presented) The system of claim 21, wherein the physical communication port is wireless.

29. (Original) The system of claim 21, wherein the client agent is associated with the security policy by loading the security policy into the client agent.

30. (Original) The system of claim 21, wherein the security manager is operable to verify that the security policy loaded into the client agent has not been modified.

31. (Previously Presented) The system of claim 21, wherein the client agent is further operative to transmit a report to a security server, the report identifying events that occurred with the computer in view of the security policy.

32. (Previously Presented) The system of claim 21, wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with the hardware device, wherein the hardware device is selected from a group consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle.

33. (Original) The system of claim 21, wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols.

34. (Previously Presented) A computer having installed thereon a module operative to:

obtain at least a portion of a data transfer passing through at least one physical communication port of the computer;

analyze said at least a portion of the data transfer according to a communication protocol associated with the at least one physical communication port; and

determine whether the data transfer is allowable based, at least in part, on the analysis of the at least a portion of the data transfer and a security policy, and, if not determining whether the data transfer is allowable, then store the at least portion of the data transfer in a buffer associated with the data transfer and wait for a subsequent data portion and, if determining the data transfer is allowable, then transferring the at least a portion of the data transfer with data stored in the associated buffer, if any exist, toward or from the physical communication port.

35. (Previously presented) The method of claim 10, wherein the device is a device selected from a group of devices consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle.

36. (Previously Presented) The method of claim 1, wherein determining whether a decision on whether to allow the data communication session may be reached is based on at least two data portions wherein at least one of said two data portions is stored in said buffer.

37. (Previously Presented) The method of claim 1, wherein determining whether to allow the data communication session is based on at least two data portions wherein at least one of said two data portions is stored in said buffer.